ROCHESTER
PUBLIC UTILITIES
WE PLEDGE, WE DELIVER™

5.B. Cyber Security Professional Development for Board Members

Rochester Public Utilities Board Meeting
November 25, 2025

Introduction to Cybersecurity in Utilities

Importance of Cybersecurity for RPU

Need for Cybersecurity

Robust cybersecurity measures are essential to protect sensitive customer data and ensure the reliability of utility services.

Public Trust

Maintaining public trust is critical for utility services, which can be achieved through strong cybersecurity practices.

Overview of Current Cyber Threat Landscape

Evolving Cyber Threats

Cyber threats are becoming more sophisticated, posing significant challenges for utilities to protect their systems.

Ransomware Attacks

Ransomware attacks, where attackers encrypt data and demand payment, have increased.

Phishing Scams

Phishing (and Vishing, Quishing) remains a major threat, tricking individuals into providing sensitive information through deceptive communications.

Denial-of-Service Attacks (DoS, or DDoS)

Denial-of-service attacks overwhelm systems, leading to downtime and disruption to crucial services for utilities.

Impact of Cyber Threats on Utility Services

Service Disruption

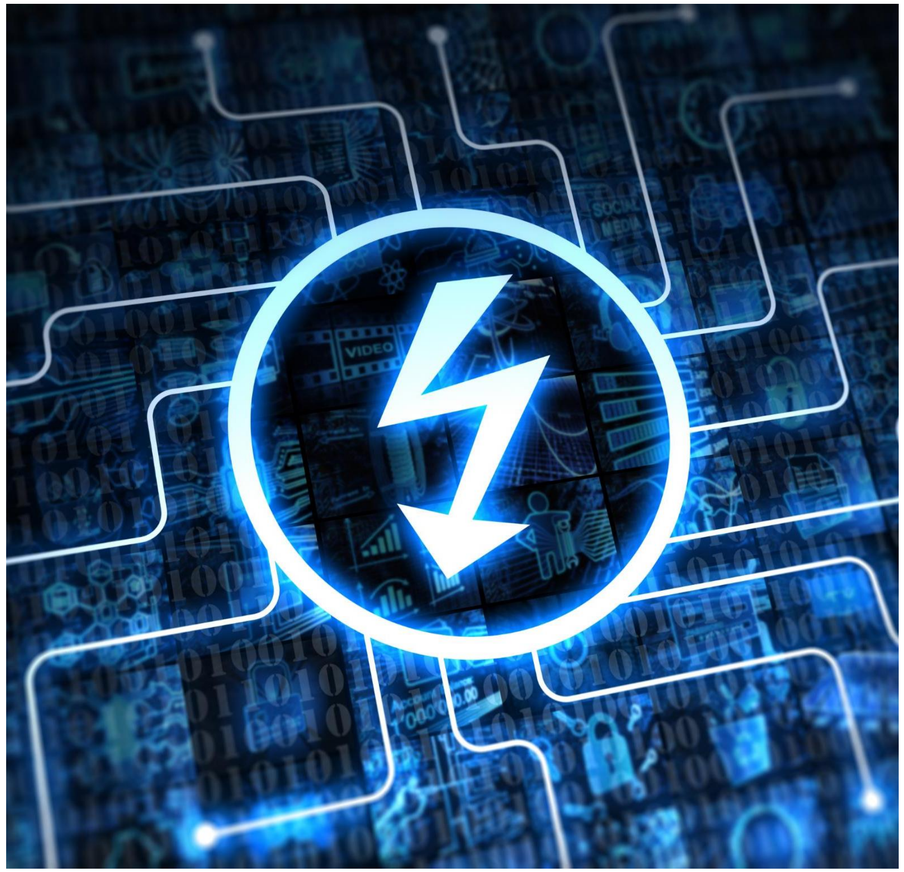
Cyber threats can lead to significant service disruptions, affecting the availability of essential utility services to customers.

Financial Losses

Utility companies can incur substantial financial losses due to cyber attacks, impacting their bottom line and operational budgets.

Reputation Damage

Cyber incidents can damage the reputation of utility providers, eroding customer trust and confidence in their ability to deliver services.



RPU’s Cybersecurity Program

Preparation for Potential Cyber Threats

TableTop eXercises (TTX)

Gather system stakeholders together against a mock incident and test out the incident response plan.

Conducting Risk Assessments

Regular risk assessments are essential for identifying vulnerabilities and strengthening the organization’s defenses against cyber threats.

Staff Training Initiatives

Training programs for staff are crucial for fostering a security-conscious culture and enhancing overall preparedness against cyber threats.

Detection Mechanisms for Cyber Threats

Monitoring Tools

Various tools are used to monitor network traffic and identify anomalies that indicate potential cyber threats.

Security Operations Center (SOC)

The SOC analyzes log files from various systems to identify patterns that match active threats (heuristics).

Detecting Anomalies (Human Brain)

Staff are trained to inform IT Security when they witness abnormal behavior or patterns that do not match traditional business and may signify a security breach.

Response Strategies to Cyber Threats

Importance of Response Strategies

Having a solid cyber incident response plan is critical during a cyber incident to align resources and protect sensitive data and systems.

RPU’s Incident Response Plan

Developed and aligned with our cyber insurance provider, the incident response plan outlines clear procedures to manage and mitigate a cyber crisis effectively.

Managing Cyber Incidents

Understand that a cyber incident response plan is a guideline and that different incidents will require different capabilities and resources. Define roles and responsibilities.

Regulatory Frameworks and Compliance

North American Electric Reliability Corporation (NERC) Compliance

Reliability Standards

NERC establishes essential standards that are crucial for the reliability of the bulk power system across North America.

Cyber Risk Protection

Compliance with NERC standards plays a vital role in protecting the bulk power system from potential cyber threats.

Alignment with National Protocols

Understanding these standards helps align RPU’s cybersecurity initiatives with established national cybersecurity protocols and frameworks.

Collaboration and Information Sharing

Enhancing Cyber Resilience / Importance of Partnerships

Collaborating with other utilities improves the overall cybersecurity resilience by sharing knowledge and resources creating a unified defense strategy across NERC entities and public power.

Information Sharing Practices

RPU participates in state/local and federal information sharing networks to significantly enhance the ability to detect threats and provide a community benefit.

Board Governance and Cybersecurity

Board Responsibilities

Cybersecurity Prioritization

Board members play a crucial role in prioritizing cybersecurity within RPU by treating cybersecurity as an enterprise risk.

Risk Management

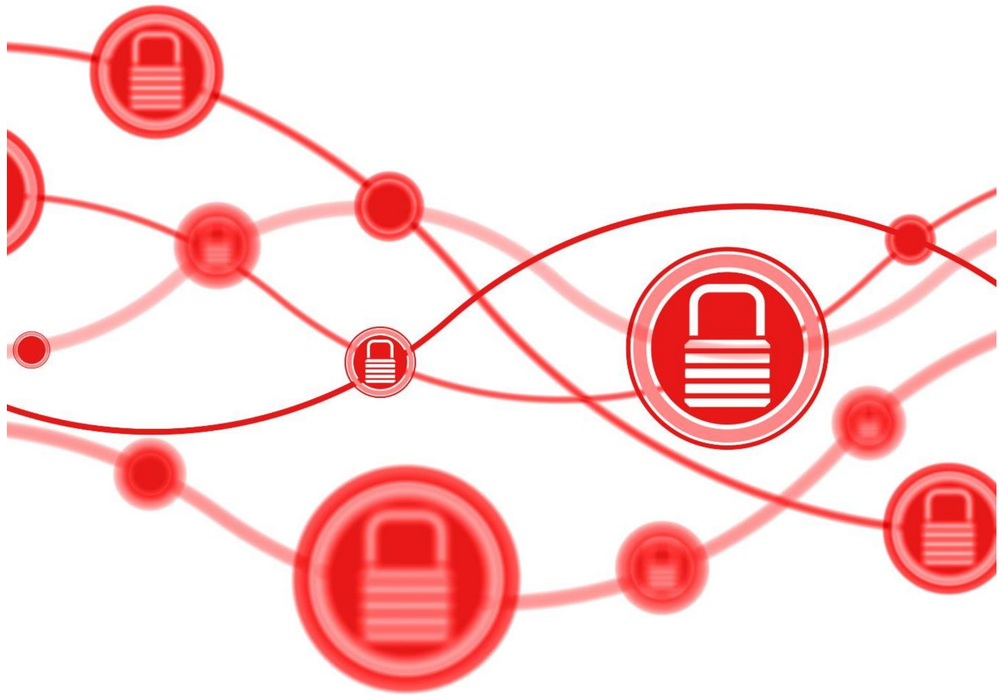
Establish and oversee RPU’s cybersecurity risk appetite, policies, and accountability

Monitor Preparedness and Response

Confirm that incident response plans are in place, tested, and include clear board communication.

Importance of Funding

Adequate funding is crucial for implementing effective cybersecurity measures and maintaining organizational resilience as cybersecurity threats evolve.



RPU’s 5 R’s (in terms of Cybersecurity)

Reliability

Reliability is inseparable from cyber protection. Hardened systems prevent outages similar to physical infrastructure upgrades.

Rates

Strong cybersecurity stabilizes rates by preventing unexpected costs that ultimately burden customers.

Responsibility

Cyber investments are part of responsible governance.

Relationships

Cyber readiness strengthens our relationships as a dependable partner and secure steward of critical community infrastructure

Reputation

RPU’s reputation is built on trust and reliability. Cybersecurity protects both.

Questions